TLP: WHITE
Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

DATE(S) ISSUED:
12/04/2019

SUBJECT:
Multiple Vulnerabilities in Mozilla Firefox Could Allow for Arbitrary Code Execution

OVERVIEW:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Mozilla Firefox is a web browser used to access the Internet. Mozilla Firefox ESR is a version of the web browser intended to be deployed in large organizations. Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user, an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

THREAT INTELLIGENCE:
There are currently no reports of these vulnerabilities being exploited in the wild.

SYSTEMS AFFECTED:
- Firefox versions prior to 71
- Firefox ESR versions prior to 68.3

RISK:
Government:
- Large and medium government entities: **High**
- Small government entities: **Medium**

Businesses:
- Large and medium business entities: **High**
- Small business entities: **Medium**

Home users: Low

TECHNICAL SUMMARY:
Multiple vulnerabilities have been discovered in Mozilla Firefox and Firefox Extended Support Release (ESR), the most severe of which could allow for arbitrary code execution. Details of the vulnerabilities are as follows:

- Heap buffer overflow in FEC processing in WebRTC (CVE-2018-6156)
- Out of bounds write in NSS when encrypting with a block cipher (CVE-2019-11745)
- Use-after-free of SFTKSession Object (CVE-2019-11756)

- Stack corruption due to incorrect number of arguments in WebRTC code (CVE-2019-13722)
- Buffer overflow in plain text serializer (CVE-2019-17005)
- Use-after-free in worker destruction (CVE-2019-17008)
- Updater temporary files accessible to unprivileged processes (CVE-2019-17009)
- Use-after-free when performing device orientation checks (CVE-2019-17010)
- Use-after-free when retrieving a document in antitracking (CVE-2019-17011)
- Memory safety bugs fixed in Firefox 71 and Firefox ESR 68.3 (CVE-2019-17012)
- Memory safety bugs fixed in Firefox 71 (CVE-2019-17013)
- Dragging and dropping a cross-origin resource, incorrectly loaded as an image, could result in information disclosure (CVE-2019-17014)

Successful exploitation of the most severe of these vulnerabilities could allow for arbitrary code execution. Depending on the privileges associated with the user an attacker could then install programs; view, change, or delete data; or create new accounts with full user rights. Users whose accounts are configured to have fewer user rights on the system could be less impacted than those who operate with administrative user rights.

RECOMMENDATIONS:
The following actions should be taken:
- Apply appropriate updates provided by Mozilla to vulnerable systems, immediately after appropriate testing.
- Run all software as a non-privileged user (one without administrative privileges) to diminish the effects of a successful attack.
- Remind users not to visit un-trusted websites or follow links provided by unknown or un-trusted sources.
- Inform and educate users regarding the threats posed by hypertext links contained in emails or attachments especially from un-trusted sources.
- Apply the Principle of Least Privilege to all systems and services.

REFERENCES:
Mozilla:
https://www.mozilla.org/en-US/security/advisories/mfsa2019-36/
https://www.mozilla.org/en-US/security/advisories/mfsa2019-37/

CVE:
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11745
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-11756
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-13722
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17005
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17008
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17009
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17010
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17011
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17012
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17013
http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2019-17014

TLP: WHITE

Disclosure is not limited. Subject to standard copyright rules, TLP: WHITE information may be distributed without restriction.
http://www.us-cert.gov/tlp/

This message and attachments may contain confidential information. If it appears that this message was sent to you by mistake, any retention, dissemination, distribution or copying of this message and attachments is strictly prohibited. Please notify the sender immediately and permanently delete the message and any attachments.

Chris Watts
Security Operations Analyst
MS Department of Information Technology Services
601-432-8201 | www.its.ms.gov

ITS Mississippi Department of
Information Technology Services

3771 Eastwood Drive | Jackson, Mississippi 39211-6381